AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1   1. (Previously presented) A method for managing a database system,

2   wherein the database system has administrators and security officers, comprising:

3   receiving a command to perform an administrative function involving an

4   object defined within the database system;

5   determining if the object is a sensitive object that is associated with

6   security functions in the database system, wherein the sensitive object is encrypted

7   in the database system, wherein the sensitive object can include a sensitive row

8   within a table in the database system, wherein the sensitive row contains sensitive

9   data, and wherein other rows in the table need not contain sensitive data;

10   wherein the sensitive object is an object that represents a sensitive user of

11   the database system who is empowered to access sensitive data;

12   wherein a security officer can perform administrative functions on

13   sensitive objects;

14   wherein an administrator cannot perform administrative functions on

15   sensitive objects;

16   wherein an administrator cannot become a sensitive user and thereby

17   obtain access to sensitive objects indirectly;

18   if the object is not a sensitive object, and if the command to perform an

19   administrative function is received from an administrator, allowing the

20   administrative function to proceed; and

21   if the object is a sensitive object, and if the command is received from an

22   administrator, disallowing the administrative function.

1   2. (Previously presented) The method of claim 1, further comprising:

2

2   receiving a request to perform an operation on a data item in the database

3   system;

4   if the data item is a sensitive data item containing sensitive information

5   and if the request is received from a sensitive user who is empowered to access

6   sensitive data, allowing the operation to proceed if the sensitive user has access

7   rights to the sensitive data item; and

8   if the data item is a sensitive data item and the request is received from a

9   user who is not a sensitive user, disallowing the operation.

1   3. (Original) The method of claim 2, wherein if the data item is a sensitive

2   data item, if the operation is allowed to proceed, and if the operation involves

3   retrieval of the data item, the method further comprises decrypting the data item

4   using an encryption key after the data item is retrieved.

1   4. (Original) The method of claim 3, wherein the encryption key is stored

2   along with a table containing the data item.

1   5. (Original) The method of claim 4, wherein the encryption key is stored

2   in encrypted form.

1   6 (Canceled).

1   7. (Original) The method of claim 1, wherein if the object is not a sensitive

2   object, and if the command to perform the administrative function is received

3   from a security officer, the method further comprises allowing the security officer

4   to perform the administrative function on the object.

1   8. (Original) The method of claim 1,

2   wherein the database system includes a number of sensitive data items;

3   and

4   wherein only specific sensitive users are allowed to access a given

5   sensitive data item.

1   9. (Previously presented) A computer-readable storage medium storing

2   instructions that when executed by a computer cause the computer to perform a

3   method for managing a database system, wherein the database system has

4   administrators and security officers, the method comprising:

5   receiving a command to perform an administrative function involving an

6   object defined within the database system;

7   determining if the object is a sensitive object that is associated with

8   security functions in the database system, wherein the sensitive object is encrypted

9   in the database system, wherein the sensitive object can include a sensitive row

10 within a table in the database system, wherein the sensitive row contains sensitive

11 data, and wherein other rows in the table need not contain sensitive data;

12   wherein the sensitive object is an object that represents a sensitive user of

13 the database system who is empowered to access sensitive data;

14   wherein a security officer can perform administrative functions on

15 sensitive objects;

16   wherein an administrator cannot perform administrative functions on

17 sensitive objects;

18   wherein an administrator cannot become a sensitive user and thereby

19 obtain access to sensitive objects indirectly;

20   if the object is not a sensitive object, and if the command is received from

21 an administrator, allowing the administrative function to proceed; and

4

22   if the object is a sensitive object, and if the command is received from an

23   administrator, disallowing the administrative function.

1   10. (Previously presented) The computer-readable storage medium of

2   claim 9, wherein the method further comprises:

3   receiving a request to perform an operation on a data item in the database

4   system;

5   if the data item is a sensitive data item containing sensitive information

6   and if the request is received from a sensitive user who is empowered to access

7   sensitive data, allowing the operation to proceed if the sensitive user has access

8   rights to the sensitive data item; and

9   if the data item is a sensitive data item and the request is received from a

10   user system who is not a sensitive user, disallowing the operation.

1   11. (Original) The computer-readable storage medium of claim 10,

2   wherein if the data item is a sensitive data item, if the operation is allowed to

3   proceed, and if the operation involves retrieval of the data item, the method

4   further comprises decrypting the data item using an encryption key after the data

5   item is retrieved.

1   12. (Original) The computer-readable storage medium of claim 11,

2   wherein the encryption key is stored along with a table containing the data item.

1   13. (Original) The computer-readable storage medium of claim 12,

2   wherein the encryption key is stored in encrypted form.

1   14 (Canceled).

5

1   15. (Original) The computer-readable storage medium of claim 9, wherein

2   if the object is not a sensitive object, and if the command to perform the

3   administrative function is received from a security officer, the method further

4   comprises allowing the security officer to perform the administrative function.

1   16. (Original) The computer-readable storage medium of claim 9,

2   wherein the database system includes a number of sensitive data items;

3   and

4   wherein only specific sensitive users are allowed to access a given

5   sensitive data item.

1   17. (Previously presented) An apparatus for managing a database system,

2   wherein the database system has administrators and security officers, comprising:

3   a command receiving mechanism that is configured to receive a command

4   to perform an administrative function involving an object defined within the

5   database system;

6   an execution mechanism that is configured to,

7   determine if the object is a sensitive object that is

8   associated with security functions in the database system, wherein

9   the sensitive object is encrypted in the database system, wherein

10   the sensitive object can include a sensitive row within a table in the

11   database system, wherein the sensitive row contains sensitive data,

12   and wherein other rows in the table need not contain sensitive data,

13   wherein the sensitive object is an object that represents a sensitive

14   user of the database system who is empowered to access sensitive

15   data;

6

16   wherein a security officer can perform administrative functions on

17 sensitive objects;

18   wherein an administrator cannot perform administrative functions on

19 sensitive objects;

20   wherein an administrator cannot become a sensitive user and thereby

21 obtain access to sensitive objects indirectly;

22   allow the administrative function to proceed, if the object is

23   not a sensitive object, and if the command is received from an

24   administrator, and to

25   disallow the administrative function, if the object is the

26   sensitive object, and if the command is received from an

27   administrator.

1   18. (Previously presented) The apparatus of claim 17,

2   wherein the command receiving mechanism is configured to receive a

3 request to perform an operation on a data item in the database system;

4   wherein the execution mechanism is configured to,

5   allow the operation to proceed, if the data item is a

6   sensitive data item, if the request is received from a sensitive user

7   who is empowered to access sensitive data, and if the sensitive user

8   has access rights to the sensitive data item, and to

9   disallow the operation, if the data item is a sensitive data

10   item, and if the request is received from a user who is not a

11   sensitive user.

1   19. (Original) The apparatus of claim 18, further comprising a decryption

2 mechanism, wherein if the data item is a sensitive data item, if the operation is

3   allowed to proceed, and if the operation involves retrieval of the data item, the

4   decryption mechanism is configured to decrypt the data item using an encryption

5   key after the data item is retrieved

1   20. (Original) The apparatus of claim 19, wherein the encryption key is

2   stored along with a table containing the data item.

1   21. (Original) The apparatus of claim 20, wherein the encryption key is

2   stored in encrypted form.

1   22 (Canceled).

1   23. (Original) The apparatus of claim 17, wherein if the object is not a

2   sensitive object, and if the command to perform the administrative function is

3   received from a security officer, the execution mechanism is configured to allow

4   the security officer to perform the administrative function.

1   24. (Original) The apparatus of claim 17,

2   wherein the database system includes a number of sensitive data items;

3   and

4   wherein only specific sensitive users are allowed to access a given

5   sensitive data item.

1   25. (Previously presented) A method for managing a database system

2   which has administrators and security officers, comprising:

3   receiving a command to perform an administrative function involving an

4   object defined within the database system;

8

5   determining if the object is a sensitive object that is associated with

6 security functions in the database system, wherein the sensitive object is an object

7 that represents a sensitive user of the database system who is empowered to access

8 sensitive data;

9   wherein a security officer can perform administrative functions on

10 sensitive objects;

11   wherein an administrator cannot perform administrative functions on

12 sensitive objects;

13   wherein an administrator cannot become a sensitive user and thereby

14 obtain access to sensitive objects indirectly;

15   if the object is not a sensitive object, and if the command is received from

16 a database administrator, allowing the administrative function to proceed; and

17   if the object is a sensitive object, and if the command is received from an

18 administrator, disallowing the administrative function.

1   26. (Previously presented) The method of claim 25, further comprising:

2   receiving a request to perform an operation on a data item in the database

3 system;

4   if the data item is a sensitive data item containing sensitive information

5 and if the request is received from a sensitive user who is empowered to access

6 sensitive data, allowing the operation to proceed if the sensitive user has access

7 rights to the sensitive data item; and

8   if the data item is a sensitive data item and the request is received from a

9 user who is not a sensitive user, disallowing the operation.

1   27. (Previously presented) The method of claim 26, wherein if the data

2 item is a sensitive data item, if the operation is allowed to proceed, and if the

9

3   operation involves retrieval of the data item, the method further comprises

4   decrypting the data item using an encryption key after the data item is retrieved.

1   28. (Previously presented) The method of claim 27, wherein the encryption

2   key is stored along with a table containing the data item.

1   29. (Previously presented) The method of claim 28, wherein the encryption

2   key is stored in encrypted form.

1   30. (Previously presented) The method of claim 25, wherein the sensitive

2   object can include one of:

3   a sensitive table containing sensitive data in the database system;

4   a sensitive row within a table in the database system, wherein the sensitive

5   row contains sensitive data; and

6   an object that represents a sensitive user of the database system who is

7   empowered to access sensitive data.

1   31. (Previously presented) The method of claim 25, wherein if the object is

2   not a sensitive object, and if the command to perform the administrative function

3   is received from a security officer, the method further comprises allowing the

4   security officer to perform the administrative function on the object.

1   32. (Previously presented) The method of claim 25,

2   wherein the database system includes a number of sensitive data items;

3   and

4   wherein only specific sensitive users are allowed to access a given

5   sensitive data item.

1   33. (Previously presented) A computer-readable storage medium storing

2   instructions that when executed by a computer cause the computer to perform a

3   method for managing a database system which has administrators and security

4   officers, the method comprising:

5   receiving a command to perform an administrative function involving an

6   object defined within the database system;

7   determining if the object is a sensitive object that is associated with

8   security functions in the database system, wherein the sensitive object is an object

9   that represents a sensitive user of the database system who is empowered to access

10   sensitive data;

11   wherein a security officer can perform administrative functions on

12   sensitive objects;

13   wherein an administrator cannot perform administrative functions on

14   sensitive objects;

15   wherein an administrator cannot become a sensitive user and thereby

16   obtain access to sensitive objects indirectly;

17   if the object is not a sensitive object, and if the command is received from

18   an administrator, allowing the administrative function to proceed; and

19   if the object is a sensitive object, and if the command is received from an

20   administrator, disallowing the administrative function.

1   34. (Previously presented) The computer-readable storage medium of

2   claim 33, wherein the method further comprises:

3   receiving a request to perform an operation on a data item in the database

4   system;

5   if the data item is a sensitive data item containing sensitive information

6   and if the request is received from a sensitive user who is empowered to access

11

7   sensitive data, allowing the operation to proceed if the sensitive user has access

8   rights to the sensitive data item; and

9   if the data item is a sensitive data item and the request is received from a

10   user who is not a sensitive user, disallowing the operation.

1   35. (Previously presented) The computer-readable storage medium of

2   claim 34, wherein if the data item is a sensitive data item, if the operation is

3   allowed to proceed, and if the operation involves retrieval of the data item, the

4   method further comprises decrypting the data item using an encryption key after

5   the data item is retrieved.

1   36. (Previously presented) The computer-readable storage medium of

2   claim 35, wherein the encryption key is stored along with a table containing the

3   data item.

1   37. (Previously presented) The computer-readable storage medium of

2   claim 36, wherein the encryption key is stored in encrypted form.

1   38. (Previously presented) The computer-readable storage medium of

2   claim 33, wherein the sensitive object can include one of:

3   a sensitive table containing sensitive data in the database system;

4   a sensitive row within a table in the database system, wherein the sensitive

5   row contains sensitive data; and

6   an object that represents a sensitive user of the database system who is

7   empowered to access sensitive data.

1   39. (Previously presented) The computer-readable storage medium of

2   claim 33, wherein if the object is not a sensitive object, and if the command to

3   perform the administrative function is received from a security officer, the method

4   further comprises allowing the security officer to perform the administrative

5   function.

1   40. (Previously presented) The computer-readable storage medium of

2   claim 33,

3   wherein the database system includes a number of sensitive data items;

4   and

5   wherein only specific sensitive users are allowed to access a given

6   sensitive data item.

1   41. (Previously presented) An apparatus for managing a database system

2   which has administrators and security officers, comprising:

3   a command receiving mechanism that is configured to receive a command

4   to perform an administrative function involving an object defined within the

5   database system;

6   wherein a security officer can perform administrative functions on

7   sensitive objects;

8   wherein an administrator cannot perform administrative functions on

9   sensitive objects;

10   wherein an administrator cannot become a sensitive user and thereby

11   obtain access to sensitive objects indirectly;

12   an execution mechanism that is configured to,

13   determine if the object is a sensitive object that is

14   associated with security functions in the database system, wherein

13

15   the sensitive object is an object that represents a sensitive user of

16   the database system who is empowered to access sensitive data,

17   allow the administrative function to proceed, if the object is

18   not a sensitive object, and if the command is received from an

19   administrator, and to

20   disallow the administrative function, if the object is a

21   sensitive object, and if the command is received from an

22   administrator.

1   42. (Previously presented) The apparatus of claim 41,

2   wherein the command receiving mechanism is configured to receive a

3 request to perform an operation on a data item in the database system;

4   wherein the execution mechanism is configured to,

5   allow the operation to proceed, if the data item is a sensitive data item, if

6 the request is received from a sensitive user who is empowered to access sensitive

7 data, and if the sensitive user has access rights to the sensitive data item, and to

8   disallow the operation, if the data item is a sensitive data item, and if the

9 request is received from a user who is not a sensitive user.

1   43. (Previously presented) The apparatus of claim 42, further comprising a

2 decryption mechanism, wherein if the data item is a sensitive data item, if the

3 operation is allowed to proceed, and if the operation involves retrieval of the data

4 item, the decryption mechanism is configured to decrypt the data item using an

5 encryption key after the data item is retrieved

1   44. (Previously presented) The apparatus of claim 43, wherein the

2 encryption key is stored along with a table containing the data item.

1   45. (Previously presented) The apparatus of claim 44, wherein the

2   encryption key is stored in encrypted form.

1   46. (Previously presented) The apparatus of claim 41, wherein the

2   sensitive object can include one of:

3   a sensitive table containing sensitive data in the database system;

4   a sensitive row within a table in the database system, wherein the sensitive

5   row contains sensitive data; and

6   an object that represents a sensitive user of the database system who is

7   empowered to access sensitive data.

1   47. (Previously presented) The apparatus of claim 41, wherein if the object

2   is not a sensitive object, and if the command to perform the administrative

3   function is received from a security officer, the execution mechanism is

4   configured to allow the security officer to perform the administrative function.

1   48. (Previously presented) The apparatus of claim 41,

2   wherein the database system includes a number of sensitive data items;

3   and

4   wherein only specific sensitive users are allowed to access a given

5   sensitive data item.